IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL BRIEF FOR THE APPELLANT

Ex parte Jeremey BARRETT, *et al.*

SYSTEM AND METHOD FOR MANAGING A PROXY REQUEST OVER A SECURE NETWORK USING INHERITED SECURITY ATTRIBUTES

Serial No. 10/748,845
Appeal No.:
Group Art Unit: 2145

Enclosed is a check in the amount of Five Hundred Ten Dollars ($970.00) to cover the official fee for this Appeal Brief and two-month Petition for Extension of Time. In the event that there may be any fees due with respect to the filing of this paper, please charge Deposit Account No. 50-2222.

Brad Y. Chin
Attorney for Appellant(s)
Reg. No. 52,738

SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Tysons Corner, VA 22182-2700

Atty. Docket: 059864.00876

BYC/dlh

Encls: Check No. 017928
Appeal Brief
Petition for Extension of Time

02/07/2008 CNGUYEN2 00000006 10748845
02 FC:1402 510.00 OP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Appellant:

Jeremey BARRETT, *et al.* Appeal No.:

Serial Number: 10/748,845 Group Art Unit: 2762

Filed: December 29, 2003 Examiner: Bhatia, Ajay M.

For: SYSTEM AND METHOD FOR MANAGING A PROXY REQUEST OVER A SECURE NETWORK USING INHERITED SECURITY ATTRIBUTES

BRIEF ON APPEAL

February 6, 2008

I. INTRODUCTION

This is an appeal from the final rejection set forth in an Official Action dated March 16, 2007, finally rejecting claims 1-28, all of the claims pending in this application, as being unpatentable over Spacey (U.S. Patent Publication No. 2002/0038371). A Request for Reconsideration was timely filed on July 16, 2007 with Petition for Extension of Time. An Advisory Action was issued on July 24, 2007, indicating that the response that was filed on July 16, 2007, did not place the application into condition for allowance. Therefore, claims 1-28 remain rejected. A Notice of Appeal and Pre-Appeal Brief Request for Review were timely filed on August 16, 2007. A Notice of Panel Decision from Pre-Appeal Brief Review was issued on November 6, 2007, indicating that the rejections of claims 1-28 were maintained. Accordingly, this Appeal Brief is being timely filed.

II. REAL PARTY IN INTEREST

The real parties in interest in this application is Nokia, Inc. of Irving, Texas, by virtue of an Assignment by the inventors, which assignment was recorded at Reel 015399, Frame 0373, on May 26, 2004.

III. STATEMENT OF RELATED APPEALS AND INTERFERENCES

There are no known related appeals and/or interferences which will directly effect or be directly effected by or have a bearing on the Board's decision in this appeal.

IV. STATUS OF CLAIMS

Claims 1-28, all of the claims pending in the present application are the subject of this appeal. Claim 1-28 were rejected under 35 U.S.C. §102(b) as being anticipated by Spacey (U.S. Patent Publication No. 2002/0038371) ("Spacey").

V. STATUS OF AMENDMENTS

No amendments were made after the final rejection.

VI. SUMMARY OF THE INVENTION

Claim 1, upon which claims 2-6 depend, recites a network device for managing a communication over a network (See Specification at least at page 4, line 16, to page 5, line 3; page 8, line 20, to page 12, line 10; page 14, line 26, to page 17, line 2). A transceiver (proxy client 210) is configured to send and to receive the communication

over the network (See Specification at least in Figures 1-5; page 8, lines 20-24; page 9, lines 8-14). A processor (access control service 214), coupled to the transceiver, is configured to receive a proxy request from a client (proxy client 210) through a secure tunnel (secure tunnel 204) (See Specification at least at page 9, lines 8-14). The processor is further configured to modify the proxy request to include a security attribute inherent from the secure tunnel (See Specification at least on page 11, lines 1-5). The modified proxy request is forwarded to a proxy service (proxy service 216) (See Specification at least on page 11, lines 1-5). The security attribute enables a proxy connection through the secure tunnel (See Specification at least on page 11, lines 6-11).

Claim 7, upon which claims 8 and 9 depend, recites an apparatus for managing a communication over a network (See Specification at least at page 4, line 16, to page 5, line 3; page 8, line 20, to page 12, line 10; page 14, line 26, to page 17, line 2). A transceiver (proxy client 210) is configured to send and to receive the communication over the network (See Specification at least in Figures 1-5; page 8, lines 20-24; page 9, lines 8-14). A processor (access control service 214), coupled to the transceiver, is configured to establish a secure tunnel (secure tunnel 204) between the apparatus and a client (proxy client 210). A proxy request is received from the client through the secure tunnel (See Specification at least at page 9, lines 8-14). The proxy request is modified to include a security attribute inherent from the secure tunnel (See Specification at least on page 11, lines 1-5). The modified proxy request is forwarded to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel (See Specification at least on page 11, lines 6-11).

Claim 10, upon which claims 11-17 depend, recites a method for managing a

communication over a network (See Specification at least at page 4, line 16, to page 5, line 3; page 8, line 20, to page 12, line 10; page 14, line 26, to page 17, line 2). A proxy request is received from a client through a secure tunnel (See Figure 5 – Block 504; See Specification at least on page 15, lines 17-27). The proxy request is modified to include a security attribute (See Figure 5 – Block 508; See Specification at least on page 16, lines 5-13). The modified proxy request is forwarded to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel (See Specification at least on page 16, lines 14-19).

Claims 18, upon which claims 19-26 depend, recites a system for managing a communication over a network (See Specification at least at page 4, line 16, to page 5, line 3; page 8, line 20, to page 12, line 10; page 14, line 26, to page 17, line 2). A client (secure tunnel client 212) is configured to determine a secure tunnel (secure tunnel 204), and send a proxy request through the determined secure tunnel (See Specification on at least page 9, lines 15-22). A server (access control service 214), coupled to the client, is configured to receive the proxy request from the client through the secure tunnel, and modify the proxy request to include a security attribute inherent from the secure tunnel (See Specification at least on page 11, lines 1-5). The server is further configured to forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel (See Specification at least on page 11, lines 6-11).

Claim 27, upon which claim 28 depends, recites an apparatus for managing a communication over a network (See Specification at least at page 4, line 16, to page 5, line 3; page 8, line 20, to page 12, line 10; page 14, line 26, to page 17, line 2). A

transceiver (proxy client 210) arranged to send and to receive the communication over the network (See Specification at least in Figures 1-5; page 8, lines 20-24; page 9, lines 8-14). A processor (access control service 214), coupled to the transceiver, is configured to receive a proxy request from a client through a secure tunnel (secure tunnel 204). A means for modifying the proxy request (access control service 214) is configured to include a security attribute inherent from the secure tunnel (See Specification at least on page 11, lines 1-5). The apparatus further includes a means for forwarding (access control service 214) the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel (See Specification at least on page 11, lines 1-11).

VII. GROUPING OF CLAIMS

The grounds of rejection to be reviewed on appeal are the rejection of claims 1-28 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2002/0038371, as applied for by Spacey ("Spacey").

VIII. APPELLANT'S ARGUMENTS

Appellants respectfully submit that each of pending claims 1-28 recites subject matter that is not taught, disclosed, or suggested by the cited art. Each of the claim is being argued separately, and thus, each of the claims stands or falls alone.

A. Claims 1-28 are novel in view of Spacey

In the Final Office Action of March 16, 2007, claims 1-28 were rejected under 35

U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2002/0038371, as applied for by Spacey ("Spacey"). Appellants respectfully submit that each of claims 1-28 recite subject matter that is not taught, disclosed, or suggested by Spacey, and as such, the Board's reversal of the rejections is respectfully requested.

1) Claim 1

Claim 1 recites a network device for managing a communication over a network. A transceiver is configured to send and to receive the communication over the network. A processor, coupled to the transceiver, is configured to receive a proxy request from a client through a secure tunnel. The processor is further configured to modify the proxy request to include a security attribute inherent from the secure tunnel. The modified proxy request is forwarded to a proxy service. The security attribute enables a proxy connection through the secure tunnel.

Appellants respectfully submit that claim 1 recites subject matter which is neither disclosed nor suggested by Spacey.

Spacey is directed to a method allowing communications to pass between private network segments without the need for holes in the firewalls of those networks. The method uses an intermediary machine located somewhere on a public network as described herein. A component in the private service network opens one or more outbound connections to the Intermediary and leaves these connections open waiting for a response. These outbound connections pass transparently through any restrictive firewalls on the private service network since these firewalls are typically set-up to block only unprompted inbound requests. A component on the client private network then connects to the same Intermediary with an outbound connection and sends it a request

that should be serviced by a server located on the otherwise inaccessible private service network. The Intermediary passes this client request on to the private service network as a response to the waiting outbound connection previously opened by the service network component to the Intermediary. The client request thus enters the private service network a response to a previously opened outbound connection from the service component and so, is not blocked by the private service networks firewall. The service component reformats the request and transmits it on to the service machine in the private network as required.

Appellants note that a "claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Additionally, the "identical invention must be shown in as complete detail as is contained in the...claim" Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellants submit that the Final Office Action has failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 1. For example, Spacey fails to disclose or suggest, at least, "a processor, coupled to the transceiver, that is configured to...modify the proxy request to include a security attribute inherent from the secure tunnel; and forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 1.

Spacey, on the other hand, merely discloses an optional encapsulation of the datagram client request in a network packet that is routable to the intermediary, whereby

the client sends a network layer request to the address of the destination service application located on a different network element or subnet (See Figs. 6 and 8 and paragraphs [0122] – [0127]). Thus, Spacey does not disclose or suggest modifying the datagram with a security attribute inherent from the secure tunnel, and then forwarding a modified datagram. In other words, in Spacey, the datagram is not modified with the security attribute while passing through the secure tunnel, then forwarded to the proxy service.

Citing paragraph [0016] of the disclosure of Spacey, the Final Office Action appears to have taken the position that Spacey discloses the aforementioned features recited in claim 1. However, paragraph [0016] of Spacey merely mentions that Spacey "differs from any existing VPN including (. . . L2F, L2TP . . .) in that communication is via an intermediary and in that, the proxy client and optional modified router component, are preferably required on each network or machine."

Accordingly, Applicants respectfully submit that Spacey does not disclose or suggest the features recited in claim 1 because the deficiency still remains that the datagram, disclosed in Spacey, is not modified with the security attributes while passing through the secure tunnel, and then forwarded to the proxy service, as clearly disclosed in the pending claims. This deficiency is further evident in that Spacey is teaching away from the use of a L2TP encapsulation because of its use of an intermediary (Spacey, paragraphs [0016] and [0122] – [0124]).

Therefore, for at least the reasons discussed above, Appellants respectfully submit that Spacey fails to disclose or suggest, at least, "a processor, coupled to the transceiver, that is configured...to modify the proxy request to include a security attribute

inherent from the secure tunnel; and forward the modified proxy request to a proxy service" as recited in claim 1. Accordingly, Appellants respectfully assert that the Final Office Action failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 1. As such, reconsideration and withdrawal of the rejection of claim 1 is respectfully requested.

2) Claim 2

Claim 2 is dependent upon claim 1, and recites further limitations. Thus, claim 2 is patentable for at least the reasons claim 1 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 2 be allowed.

3) Claim 3

Claim 3 is dependent upon claim 1, and recites further limitations. Thus, claim 3 is patentable for at least the reasons claim 1 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 3 be allowed.

4) Claim 4

Claim 4 is dependent upon claim 1, and recites further limitations. Thus, claim 4 is patentable for at least the reasons claim 1 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 4 be allowed.

5) Claim 5

Claim 5 is dependent upon claim 1, and recites further limitations. Thus, claim 5 is patentable for at least the reasons claim 1 is patentable, and further, because it recites

additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 5 be allowed.

6) Claim 6

Claim 6 is dependent upon claim 1, and recites further limitations. Thus, claim 6 is patentable for at least the reasons claim 1 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 6 be allowed.

7) Claim 7

Claim 7 recites an apparatus for managing a communication over a network. A transceiver is configured to send and to receive the communication over the network. A processor, coupled to the transceiver, is configured to establish a secure tunnel between the apparatus and a client. A proxy request is received from the client through the secure tunnel. The proxy request is modified to include a security attribute inherent from the secure tunnel. The modified proxy request is forwarded to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

Appellants respectfully submit that claim 7 recites subject matter which is neither disclosed nor suggested by Spacey.

Spacey is directed to a method allowing communications to pass between private network segments without the need for holes in the firewalls of those networks. The method uses an intermediary machine located somewhere on a public network as described herein. A component in the private service network opens one or more outbound connections to the Intermediary and leaves these connections open waiting for a response. These outbound connections pass transparently through any restrictive

firewalls on the private service network since these firewalls are typically set-up to block only unprompted inbound requests. A component on the client private network then connects to the same Intermediary with an outbound connection and sends it a request that should be serviced by a server located on the otherwise inaccessible private service network. The Intermediary passes this client request on to the private service network as a response to the waiting outbound connection previously opened by the service network component to the Intermediary. The client request thus enters the private service network a response to a previously opened outbound connection from the service component and so, is not blocked by the private service networks firewall. The service component reformats the request and transmits it on to the service machine in the private network as required.

Appellants note that a "claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Additionally, the "identical invention must be shown in as complete detail as is contained in the...claim" Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellants submit that the Final Office Action has failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 7. For example, Spacey fails to disclose or suggest, at least, "a processor, coupled to the transceiver, that is configured to...modify the proxy request to include a security attribute inherent from the secure tunnel; and forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure

tunnel" as recited in claim 7.

Spacey, on the other hand, merely discloses an optional encapsulation of the datagram client request in a network packet that is routable to the intermediary, whereby the client sends a network layer request to the address of the destination service application located on a different network element or subnet (See Figs. 6 and 8 and paragraphs [0122] – [0127]). Thus, Spacey does not disclose or suggest modifying the datagram with a security attribute inherent from the secure tunnel, and then forwarding a modified datagram. In other words, in Spacey, the datagram is not modified with the security attribute while passing through the secure tunnel, then forwarded to the proxy service.

Citing paragraph [0016] of the disclosure of Spacey, the Final Office Action appears to have taken the position that Spacey discloses the aforementioned features recited in claim 7. However, paragraph [0016] of Spacey merely mentions that Spacey "differs from any existing VPN including (. . . L2F, L2TP . . .) in that communication is via an intermediary and in that, the proxy client and optional modified router component, are preferably required on each network or machine."

Accordingly, Applicants respectfully submit that Spacey does not disclose or suggest the features recited in claim 7 because the deficiency still remains that the datagram, disclosed in Spacey, is not modified with the security attributes while passing through the secure tunnel, and then forwarded to the proxy service, as clearly disclosed in the pending claims. This deficiency is further evident in that Spacey is teaching away from the use of a L2TP encapsulation because of its use of an intermediary (Spacey, paragraphs [0016] and [0122] – [0124]).

Therefore, for at least the reasons discussed above, Appellants respectfully submit that Spacey fails to disclose or suggest, at least, "a processor, coupled to the transceiver, that is configured to...modify the proxy request to include a security attribute inherent from the secure tunnel; and forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 7. Accordingly, Appellants respectfully assert that the Final Office Action failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 7. As such, reconsideration and withdrawal of the rejection of claim 7 is respectfully requested.

8) Claim 8

Claim 8 is dependent upon claim 7, and recites further limitations. Thus, claim 8 is patentable for at least the reasons claim 7 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 8 be allowed.

9) Claim 9

Claim 9 is dependent upon claim 7, and recites further limitations. Thus, claim 9 is patentable for at least the reasons claim 7 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 9 be allowed.

10) Claim 10

Claim 10 recites a method for managing a communication over a network. A proxy request is received from a client through a secure tunnel. The proxy request is modified to include a security attribute. The modified proxy request is forwarded to a proxy service,

wherein the security attribute enables a proxy connection through the secure tunnel.

Appellants respectfully submit that claim 10 recites subject matter which is neither disclosed nor suggested by Spacey.

Spacey is directed to a method allowing communications to pass between private network segments without the need for holes in the firewalls of those networks. The method uses an intermediary machine located somewhere on a public network as described herein. A component in the private service network opens one or more outbound connections to the Intermediary and leaves these connections open waiting for a response. These outbound connections pass transparently through any restrictive firewalls on the private service network since these firewalls are typically set-up to block only unprompted inbound requests. A component on the client private network then connects to the same Intermediary with an outbound connection and sends it a request that should be serviced by a server located on the otherwise inaccessible private service network. The Intermediary passes this client request on to the private service network as a response to the waiting outbound connection previously opened by the service network component to the Intermediary. The client request thus enters the private service network a response to a previously opened outbound connection from the service component and so, is not blocked by the private service networks firewall. The service component reformats the request and transmits it on to the service machine in the private network as required.

Appellants note that a "claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051,

1053 (Fed. Cir. 1987). Additionally, the "identical invention must be shown in as complete detail as is contained in the...claim" Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellants submit that the Final Office Action has failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 10. For example, Spacey fails to disclose or suggest, at least, "modifying the proxy request to include a security attribute; and forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 10.

Spacey, on the other hand, merely discloses an optional encapsulation of the datagram client request in a network packet that is routable to the intermediary, whereby the client sends a network layer request to the address of the destination service application located on a different network element or subnet (See Figs. 6 and 8 and paragraphs [0122] – [0127]). Thus, Spacey does not disclose or suggest modifying the datagram with a security attribute inherent from the secure tunnel, and then forwarding a modified datagram. In other words, in Spacey, the datagram is not modified with the security attribute while passing through the secure tunnel, then forwarded to the proxy service.

Citing paragraph [0016] of the disclosure of Spacey, the Final Office Action appears to have taken the position that Spacey discloses the aforementioned features recited in claim 10. However, paragraph [0016] of Spacey merely mentions that Spacey "differs from any existing VPN including (. . . L2F, L2TP . . .) in that communication is via an intermediary and in that, the proxy client and optional modified router component, are

preferably required on each network or machine."

Accordingly, Applicants respectfully submit that Spacey does not disclose or suggest the features recited in claim 10 because the deficiency still remains that the datagram, disclosed in Spacey, is not modified with the security attributes while passing through the secure tunnel, and then forwarded to the proxy service, as clearly disclosed in the pending claims. This deficiency is further evident in that Spacey is teaching away from the use of a L2TP encapsulation because of its use of an intermediary (Spacey, paragraphs [0016] and [0122] – [0124]).

Therefore, for at least the reasons discussed above, Appellants respectfully submit that Spacey fails to disclose or suggest, at least, "modifying the proxy request to include a security attribute; and forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 10. Accordingly, Appellants respectfully assert that the Final Office Action failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 10. As such, reconsideration and withdrawal of the rejection of claim 10 is respectfully requested.

11) Claim 11

Claim 11 is dependent upon claim 10, and recites further limitations. Thus, claim 11 is patentable for at least the reasons claim 10 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 11 be allowed.

12) Claim 12

Claim 12 is dependent upon claim 10, and recites further limitations. Thus, claim

12 is patentable for at least the reasons claim 10 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 12 be allowed.

13) Claim 13

Claim 13 is dependent upon claim 10, and recites further limitations. Thus, claim 13 is patentable for at least the reasons claim 10 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 13 be allowed.

14) Claim 14

Claim 14 is dependent upon claim 10, and recites further limitations. Thus, claim 14 is patentable for at least the reasons claim 10 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 14 be allowed.

15) Claim 15

Claim 15 is dependent upon claim 10, and recites further limitations. Thus, claim 15 is patentable for at least the reasons claim 10 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 15 be allowed.

16) Claim 16

Claim 16 is dependent upon claim 10, and recites further limitations. Thus, claim 16 is patentable for at least the reasons claim 10 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 16 be allowed.

17) Claim 17

Claim 17 is dependent upon claim 10, and recites further limitations. Thus, claim 17 is patentable for at least the reasons claim 10 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 17 be allowed.

18) Claim 18

Claims 18 recites a system for managing a communication over a network. A client is configured to determine a secure tunnel, and send a proxy request through the determined secure tunnel. A server, coupled to the client, is configured to receive the proxy request from the client through the secure tunnel, and modify the proxy request to include a security attribute inherent from the secure tunnel. The server is further configured to forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

Appellants respectfully submit that claim 18 recites subject matter which is neither disclosed nor suggested by Spacey.

Spacey is directed to a method allowing communications to pass between private network segments without the need for holes in the firewalls of those networks. The method uses an intermediary machine located somewhere on a public network as described herein. A component in the private service network opens one or more outbound connections to the Intermediary and leaves these connections open waiting for a response. These outbound connections pass transparently through any restrictive firewalls on the private service network since these firewalls are typically set-up to block only unprompted inbound requests. A component on the client private network then

connects to the same Intermediary with an outbound connection and sends it a request that should be serviced by a server located on the otherwise inaccessible private service network. The Intermediary passes this client request on to the private service network as a response to the waiting outbound connection previously opened by the service network component to the Intermediary. The client request thus enters the private service network a response to a previously opened outbound connection from the service component and so, is not blocked by the private service networks firewall. The service component reformats the request and transmits it on to the service machine in the private network as required.

Appellants note that a "claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Additionally, the "identical invention must be shown in as complete detail as is contained in the...claim" Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellants submit that the Final Office Action has failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 18. For example, Spacey fails to disclose or suggest, at least, "a server, coupled to the client, that is configured to...modify the proxy request to include a security attribute inherent from the secure tunnel; and forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 18.

Spacey, on the other hand, merely discloses an optional encapsulation of the datagram client request in a network packet that is routable to the intermediary, whereby the client sends a network layer request to the address of the destination service application located on a different network element or subnet (See Figs. 6 and 8 and paragraphs [0122] – [0127]). Thus, Spacey does not disclose or suggest modifying the datagram with a security attribute inherent from the secure tunnel, and then forwarding a modified datagram. In other words, in Spacey, the datagram is not modified with the security attribute while passing through the secure tunnel, then forwarded to the proxy service.

Citing paragraph [0016] of the disclosure of Spacey, the Final Office Action appears to have taken the position that Spacey discloses the aforementioned features recited in claim 18. However, paragraph [0016] of Spacey merely mentions that Spacey "differs from any existing VPN including (. . . L2F, L2TP . . .) in that communication is via an intermediary and in that, the proxy client and optional modified router component, are preferably required on each network or machine."

Accordingly, Applicants respectfully submit that Spacey does not disclose or suggest the features recited in claim 18 because the deficiency still remains that the datagram, disclosed in Spacey, is not modified with the security attributes while passing through the secure tunnel, and then forwarded to the proxy service, as clearly disclosed in the pending claims. This deficiency is further evident in that Spacey is teaching away from the use of a L2TP encapsulation because of its use of an intermediary (Spacey, paragraphs [0016] and [0122] – [0124]).

Therefore, for at least the reasons discussed above, Appellants respectfully

submit that Spacey fails to disclose or suggest, at least, "a server, coupled to the client, that is configured to...modify the proxy request to include a security attribute inherent from the secure tunnel; and forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 18. Accordingly, Appellants respectfully assert that the Final Office Action failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 18. As such, reconsideration and withdrawal of the rejection of claim 18 is respectfully requested.

19) Claim 19

Claim 19 is dependent upon claim 18, and recites further limitations. Thus, claim 19 is patentable for at least the reasons claim 18 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 19 be allowed.

20) Claim 20

Claim 20 is dependent upon claim 18, and recites further limitations. Thus, claim 20 is patentable for at least the reasons claim 18 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 20 be allowed.

21) Claim 21

Claim 21 is dependent upon claim 20, and recites further limitations. Thus, claim 21 is patentable for at least the reasons claim 20 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 21 be allowed.

22) Claim 22

Claim 22 is dependent upon claim 20, and recites further limitations. Thus, claim 22 is patentable for at least the reasons claim 20 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 22 be allowed.

23) Claim 23

Claim 23 is dependent upon claim 20, and recites further limitations. Thus, claim 23 is patentable for at least the reasons claim 20 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 23 be allowed.

24) Claim 24

Claim 24 is dependent upon claim 20, and recites further limitations. Thus, claim 24 is patentable for at least the reasons claim 20 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 24 be allowed.

25) Claim 25

Claim 25 is dependent upon claim 20, and recites further limitations. Thus, claim 25 is patentable for at least the reasons claim 20 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 25 be allowed.

26) Claim 26

Claim 26 is dependent upon claim 20, and recites further limitations. Thus, claim 26 is patentable for at least the reasons claim 20 is patentable, and further, because it

recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 26 be allowed.

27) Claim 27

Claim 27 recites an apparatus for managing a communication over a network. A transceiver arranged to send and to receive the communication over the network. A processor, coupled to the transceiver, is configured to receive a proxy request from a client through a secure tunnel. A means for modifying the proxy request is configured to include a security attribute inherent from the secure tunnel. The apparatus further includes a means for forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

Appellants respectfully submit that claim 27 recites subject matter which is neither disclosed nor suggested by Spacey.

Spacey is directed to a method allowing communications to pass between private network segments without the need for holes in the firewalls of those networks. The method uses an intermediary machine located somewhere on a public network as described herein. A component in the private service network opens one or more outbound connections to the Intermediary and leaves these connections open waiting for a response. These outbound connections pass transparently through any restrictive firewalls on the private service network since these firewalls are typically set-up to block only unprompted inbound requests. A component on the client private network then connects to the same Intermediary with an outbound connection and sends it a request that should be serviced by a server located on the otherwise inaccessible private service network. The Intermediary passes this client request on to the private service network as

a response to the waiting outbound connection previously opened by the service network component to the Intermediary. The client request thus enters the private service network a response to a previously opened outbound connection from the service component and so, is not blocked by the private service networks firewall. The service component reformats the request and transmits it on to the service machine in the private network as required.

Appellants note that a "claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Additionally, the "identical invention must be shown in as complete detail as is contained in the...claim" Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellants submit that the Final Office Action has failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 27. For example, Spacey fails to disclose or suggest, at least, "a processor, coupled to the transceiver, that is configured to receive a proxy request from a client through a secure tunnel; a means for modifying the proxy request to include a security attributable inherent form the secure tunnel; and a means for forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 27.

Spacey, on the other hand, merely discloses an optional encapsulation of the datagram client request in a network packet that is routable to the intermediary, whereby the client sends a network layer request to the address of the destination service application located on a different network element or subnet (See Figs. 6 and 8 and paragraphs [0122] – [0127]). Thus, Spacey does not disclose or suggest modifying the datagram with a security attribute inherent from the secure tunnel, and then forwarding a modified datagram. In other words, in Spacey, the datagram is not modified with the security attribute while passing through the secure tunnel, then forwarded to the proxy service.

Citing paragraph [0016] of the disclosure of Spacey, the Final Office Action appears to have taken the position that Spacey discloses the aforementioned features recited in claim 27. However, paragraph [0016] of Spacey merely mentions that Spacey "differs from any existing VPN including (. . . L2F, L2TP . . .) in that communication is via an intermediary and in that, the proxy client and optional modified router component, are preferably required on each network or machine."

Accordingly, Applicants respectfully submit that Spacey does not disclose or suggest the features recited in claim 27 because the deficiency still remains that the datagram, disclosed in Spacey, is not modified with the security attributes while passing through the secure tunnel, and then forwarded to the proxy service, as clearly disclosed in the pending claims. This deficiency is further evident in that Spacey is teaching away from the use of a L2TP encapsulation because of its use of an intermediary (Spacey, paragraphs [0016] and [0122] – [0124]).

Therefore, for at least the reasons discussed above, Appellants respectfully

submit that Spacey fails to disclose or suggest, at least, "a processor, coupled to the transceiver, that is configured to receive a proxy request from a client through a secure tunnel; a means for modifying the proxy request to include a security attributable inherent form the secure tunnel; and a means for forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel" as recited in claim 27. Accordingly, Appellants respectfully assert that the Final Office Action failed to establish a *prima facie* case of anticipation as Spacey fails to disclose each and every element of claim 27. As such, reconsideration and withdrawal of the rejection of claim 27 is respectfully requested.

28) Claim 28

Claim 28 is dependent upon claim 27, and recites further limitations. Thus, claim 28 is patentable for at least the reasons claim 27 is patentable, and further, because it recites additional limitations. Accordingly, it is respectfully requested that this rejection be reversed and claim 28 be allowed.

For all of the above noted reasons, it is strongly contended that certain clear differences exist between the present invention as claimed in claims 1-28 and the prior art relied upon by the Examiner. It is further contended that these differences are more than sufficient that the present invention would not have been obvious to a person having ordinary skill in the art at the time the invention was made.

This final rejection being in error, therefore, it is respectfully requested that this honorable Board of Patent Appeals and Interferences reverse the Examiner's decision in this case and indicate the allowability of application claims 1-28.

In the event that this paper is not being timely filed, the applicant respectfully

petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees which may be due with respect to this paper may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

SQUIRE, SANDERS & DEMPSEY LLP

Brad Y. Chin
Attorney for Applicant(s)
Registration No. 52,738

Atty. Docket No.: 059864.00876

8000 Towers Crescent Drive, 14th Floor
Tysons Corner, VA 22182-2700
Tel: (703) 720-7800
Fax: (703) 720-7802

BYC:dlh

Encls: Appendix 1 - Claims on Appeal
Appendix 2 - Evidence
Appendix 3 - Related Proceedings

APPENDIX 1

CLAIMS ON APPEAL

1. (Previously Presented) A network device for managing a communication over a network, comprising:

a transceiver configured to send and to receive the communication over the network;

a processor, coupled to the transceiver, that is configured to:

receive a proxy request from a client through a secure tunnel;

modify the proxy request to include a security attribute inherent from the secure tunnel; and

forward the modified proxy request to a proxy service,

wherein the security attribute enables a proxy connection through the secure tunnel.

2. (Previously Presented) The network device of claim 1, wherein modifying the proxy request further comprises including a security header with the proxy request.

3. (Previously Presented) The network device of claim 1, wherein the security attribute further comprises at least one of an internet protocol (IP) address associated with the client, a security property associated with the secure tunnel, a pub is key certificate, a security credential associated with the client, access control data configured to enable the client access to a content server, a session identifier, and an identifier associated with the secure tunnel.

4. (Previously Presented) The network device of claim 1, wherein the proxy request is an hyper text transport protocol (HTTP) proxy request.

5. (Previously Presented) The network device of claim 1, wherein the secure tunnel further comprises at least one of a secure sockets layer (SSL) tunnel, a transport

layer security(TLS) tunnel, hyper text transport protocol (HTTP) Secure (HTTPS), Tunneling TLS (TTLS), and an extensible authentication protocol (EAP) secure tunnel.

6. (Previously Presented) The network device of claim 1, further comprising receiving an hyper text transport protocol secure (HTTPS) communication to enable the secure tunnel.

7. (Previously Presented) An apparatus for managing a communication over a network, comprising:

a transceiver configured to send and to receive the communication over the network;

a processor, coupled to the transceiver, that is configured to:

establish a secure tunnel between the apparatus and a client;

receive a proxy request from the client through the secure tunnel;

modify the proxy request to include a security attribute inherent from the secure tunnel; and

forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

8. (Previously Presented) The apparatus of claim 7, wherein establishing the secure tunnel further comprises receiving an hyper text transport secure (HTTPS) communication.

9. (Previously Presented) The apparatus of claim 7, wherein the apparatus is operable as at least one of a firewall, a gateway, and a proxy server.

10. (Original) A method for managing a communication over a network, comprising:

receiving a proxy request from a client through a secure tunnel;

modifying the proxy request to include a security attribute; and

forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

11. (Previously Presented) The method of claim 10, wherein modifying the proxy request further comprises associating a security header with the proxy request.

12. (Previously Presented) The method of claim 10, wherein the security attribute further comprises at least one of an IP address associated with the client, a security property associated with the secure tunnel, a public key certificate, access control data configured to enable the client access to a content server, a security credential associated with the client, a session identifier, and an identifier.

13. (Previously Presented) The method of claim 10, wherein the proxy request is an hyper text transport protocol (HTTP) proxy request.

14. (Previously Presented) The method of claim 10, wherein the secure tunnel further comprises at least one of an secure socket layer (SSL) tunnel, a transport layer security (TLS) tunnel, hyper text transport protocol (HTTP) Secure (HTTPS), Tunneling TLS (TTLS), IPSec tunnel, and an extensible authentication protocol (EAP) secure tunnel.

15. (Previously Presented) The method of claim 10, further comprising receiving an hyper text transport protocol secure (HTTPS) communication to enable the establishment of the secure tunnel.

16. (Previously Presented) The method of claim 10, further comprising:

initiating a connection to a secure tunnel client; and

sending the proxy request to the secure tunnel client, wherein the secure tunnel client is configured to forward the proxy request over the secure tunnel.

17. (Previously Presented) The method of claim 10, wherein modifying the proxy request further comprises modifying the proxy request employing an access control service.

18. (Previously Presented) A system for managing a communication over a network, comprising:

a client that is configured to:

determine a secure tunnel; and

send a proxy request through the determined secure tunnel; and

a server, coupled to the client, that is configured to:

receive the proxy request from the client through the secure tunnel;

modify the proxy request to include a security attribute inherent from the secure tunnel; and

forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

19. (Previously Presented) The system of claim 18, wherein the client further comprises:

a proxy client that is configured to generate a proxy request; and

a secure tunnel client, coupled to the proxy client, that is configured to establish the secure tunnel with the server.

20. (Previously Presented) The system of claim 19, wherein the proxy client further comprises a port-forwarding client application.

21. (Previously Presented) The system of claim 18, wherein modifying the proxy request further comprises including a security header with the proxy request.

22. (Previously Presented) The system of claim 18, wherein the security attribute further comprises at least one of an internet protocol (IP) address associated

with the client, a security property associated with the secure tunnel, a public key certificate, access control data configured to enable the client access to a content server, a security credential associated with the client, a session identifier, and an identifier associated with the secure tunnel.

23. (Previously Presented) The system of claim 18, wherein the proxy request is a hyper text transport protocol (HTTP) proxy request.

24. (Previously Presented) The system of claim 18, wherein the secure tunnel further comprises a means for securing the communication over the network.

25. (Previously Presented) The system of claim 18, wherein the secure tunnel further comprises at least one of a secure socket layer (SSL) tunnel, a transport layer security (TLS) tunnel, hyper text transport protocol (HTTP) Secure (HTTPS), Tunneling TLS (TTLS), IPSec tunnel, and an extensible authentication protocol (EAP) secure tunnel.

26. (Previously Presented) The system of claim 18, wherein determining the secure tunnel further comprises generating an hyper text transport protocol secure (HTTPS) message to enable the secure tunnel.

27. (Previously Presented) An apparatus for managing a communication over a network, comprising:

a transceiver arranged to send and to receive the communication over the network;

a processor, coupled to the transceiver, that is configured to receive a proxy request from a client through a secure tunnel;

a means for modifying the proxy request to include a security attribute inherent from the secure tunnel; and

a means for forwarding the modified proxy request to a proxy service, wherein the

security attribute enables a proxy connection through the secure tunnel.

28. (Previously Presented) The apparatus of claim 27, wherein the secure tunnel further comprises a means for securing the communication over the network.

APPENDIX 2

EVIDENCE APPENDIX

No evidence under section 37 C.F.R. 1.130, 1.131, or 1.132 has been entered or will be relied upon by Appellants in this appeal.

APPENDIX 3

RELATED PROCEEDINGS APPENDIX

No decisions of the Board or of any court have been identified under 37 C.F.R. §41.37(c)(1)(ii).